METHOD AND SYSTEM FOR CERTIFICATE DELIVERY AND MANAGEMENT

Priority Application

This application claims the benefit of U.S. Provisional Application No. 60/408,616 filed September 6, 2002, entitled Method and System for Certificate Delivery and Management, incorporated herein by this reference.

Field of the Invention

The present invention relates generally to the field of certificate delivery and management, and more particularly to a method and system for combining multiple access points and utilizing certificates as an access method to a system from multiple access points.

Background of the Invention

Certificate technology and certificate-based access to systems is prevalent and existent within the industry today. However, there is a present need for a specific deployment of the certificate-based access method over multiple different types of access vehicles which, for example, enables users to utilize a certificate that is stored within a smart card to access a host system through a browser, such that when the user accesses the application on the server, the application requires that the card and certificate be present for authentication of the individual user and concurrently allows systems which need access to applications on a server to use a certificate stored on that system for authentication of itself to the server.

Summary of the Invention

It is a feature and advantage of the present invention to provide a method and system for combining multiple access points and using certificates as an access method to a system from multiple access points that enables users to utilize a certificate that is stored within a smart card to access the host system through a browser.

It is a further feature and advantage of the present invention to provide a method and system for combining multiple access points and utilizing certificates as an access method to a system from multiple access points that provides access to the

entire system using certificates and populating the certificates across multiple, different storage mechanisms.

It is another feature and advantage of the present invention to provide a method and system for combining multiple access points and utilizing certificates as an access method to a system from multiple access points that manages the creation and distribution of those certificates across several different storage methods.

It is an additional feature and advantage of the present invention to provide a method and system for combining multiple access points and utilizing certificates as an access method to a system from multiple access points that provides management of the certificates over the life span of the certificate.

It is a still further feature and advantage of the present invention to provide a method and system for combining multiple access points and utilizing certificates as an access method to a system from multiple access points that provides re-issuance and revocation of certificates.

It is still another feature and advantage of the present invention to provide a method and system for combining multiple access points and utilizing certificates as an access method to a system from multiple access points that manages certificates across these multiple methods.

To achieve the stated and other features, advantages and objects, an embodiment of the present invention provides a method and system for combining multiple access points and utilizing certificates as an access method to a system from multiple access points. A specific deployment aspect of the present invention employs the certificate-based access method over multiple different types of access vehicles. Users are able to utilize a certificate that is stored within a smart card, and when they need to access the host system, through a browser, the user accesses the application on the server, and the application requires that the card and certificate be present for authentication of the individual user. In addition, other systems have rights to access the host system, also providing updated information. Both systems require the same level of access control, which means a public key-based authentication. In order to accomplish that, certificates stored on the system are also used.

Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become more apparent

to those skilled in the art upon examination of the following, or may be learned by practice of the invention.

Brief Description of the Drawings

Fig. 1 is a flow chart with illustrates an example of the process of creating and distributing a certificate for storage on the microcomputer of an integrated chip card for an embodiment of the present invention;

Fig. 2 is a flow chart with illustrates an example of the process of creating and distributing a certificate for storage on a computer disk in a secure environment for an embodiment of the present invention; and

Fig. 3 is a flow chart with illustrates an example of the process of creating and distributing a certificate for storage on a hardware storage module associated with a computer for an embodiment of the present invention.

Detailed Description

Referring now in detail to an embodiment of the invention, an example of which is illustrated in the accompanying drawings, an aspect of the present invention provides a method and system for combining multiple access points and utilizing certificates as an access method to a system from multiple access points. Certificates and public technology are prevalent and existent within the industry today. Certificate-based access to systems is something that is also existent today. However, a specific deployment aspect of an embodiment of the present invention employs the certificate-based access method over multiple different types of access vehicles. For example, users are able to utilize a certificate that is stored within a smart card, and when they need to access the host system, through a browser, the user accesses the application on the server, and the application requires that the card and certificate be present for authentication of the individual user. Fig. 1 illustrates an example of the process of creating and distributing a certificate for storage on the microcomputer of an integrated chip card, also known as a smart card, for an embodiment of the invention.

In addition, in an embodiment of the present invention, other systems have rights to access the host system, also providing updated information. Both systems require the same level of access control, which means a public key-based

authentication. In order to accomplish that, certificates stored on the system are also used. The storage mechanism is twofold. In certain systems which are in secure locations, what is called soft storage is allowed, which means that the certificates and the keys associated with a particular certificate are stored on the disk on the system. Fig. 2 illustrates an example of the process of creating and distributing a certificate for storage on a computer disk in a secure environment for an embodiment of the invention.

The other storage method is storage of the private key or certificate on a hardware security module ("HSM"). The security module is a physical component or card or external box attached to a computer that securely stores encryption keys and securely encrypts information by passing information into the module encrypting it, and then passing the encrypted information out. By doing that, the keys are never externally viewed or accessible. Fig. 3 illustrates an example of the process of creating and distributing a certificate for storage on a HSW associated with a computer for an embodiment of the present invention.

An embodiment of the present invention provides access to the entire system using certificates and populating the certificates across multiple, different storage mechanisms. This multiplicity of storage mechanisms is an important aspect of an embodiment of the present invention. Another important aspect is how the system manages the creation and distribution of those certificates across the three different storage methods. An additional important aspect is how the system manages the certificates over the life span of the certificate. Further important aspects include, for example, how the system deals with re-issuance and revocation of certificates and how the system manages certificates across these multiple methods.

In an embodiment of the present invention, different solutions are implemented to create the certificate. One method involves creating certificates for a card where an individual can interact with the card and load certificates, for example, by requesting certificates and getting them approved . In dealing with systems that require receiving certificates, there are different requirements for certificate generation. The system for an embodiment of the present invention combines both the creation and requests for certificates from systems into a single solution. While HSMs are commonly used to store key information when dealing with a host or web server environment in a network-based solution, HSMs are typically not used on the

client side to store certificates. Another important aspect of the system for an embodiment of the present invention is the integration of an HSM to store the private keys on the client side system.

Referring to Fig. 1 and the Appendix hereto, which is a document entitled "eConsumer Emerging Technologies LCMS Access Control User Guide" consisting of 71 pages for an embodiment of the present invention, which is incorporated herein in its entirety by this reference, the diagram of the Appendix labeled Appendix B and entitled "CA/RA Architecture Diagram" omits the workstation that is used to initialize the cards in an embodiment of the present invention. That workstation actually prepares the key pair for the card, as well as putting the unique PIN on the card. A PIN is used on the administrator card for users to unlock the card and then have the card's certificate available. This is standard practice in card technology, which allows the cardholder to have something that the cardholder knows is unique about the card, that is one level of authentication. In addition, the card has the information to authenticate itself to the host system with which the card is talking. By doing that, it is possible to employ less sophisticated cryptography for the cardholder himself or herself to interact with the card and more sophisticated encryption technology when dealing with authentication, signing or establishing secure communication channels in the actual interactions with the computer or across computer networks.

In an embodiment of the present invention, the cards prepared by the initial workstation are delivered to an operations center that is responsible for establishing the access control to the host system. Security administrators within that operations environment then receive requests for access. A list of requests for individuals having access to the system are processed through and identified, for example, in a couple of ways. An operations staff member gets on to the personalization system, and with the information provided, links an individual card with its PIN and key pair and creates a certificate for that cardholder. That request for a certificate goes to the Certificate Authority ("CA") system. Referring again to Fig. 1 and the Appendix hereto, which is the document entitled "eConsumer Emerging Technologies LCMS Access Control User Guide" consisting of 71 pages and incorporated herein in its entirety by this reference, of the RA/CA pair shown on the diagram entitled "CA/RA Architecture Diagram" of Appendix B of the Appendix hereto, the RA or Registration Authority is the system in which the user requests the certificate. The RA sends that request to the

CA. The CA reviews the request to see if all of the information is there and creates and signs the certificate and then has the certificate ready to place it back on the card itself.

The CA has an initial key pair that it uses to create a master certificate. That master certificate is what is used to sign the certificates that are created by the CA. That signature is what is used or verified to validate the authenticity of the certificate. A KMS or Key Management System is a separate component within the system, which is used to store master keys and then distribute them to entities. The KMS can be used in this model to be the repository of a master key for the system. It also holds master keys for many other aspects of this solution and distributes them to card vendors, to the host system, and the like, so that other aspects of cards not related to this portion of the process can be manipulated.

In an embodiment of the present invention, a certificate is created and signed, and then the card is put into the personalization workstation. The certificate is downloaded back to that part. In addition, when that is done, the CA is linked with another technology component within the host environment which is called directory services. There is an LDAP directory on the CCLMS or Card Life Cycle Management System for both the CA and the CCLMS. The CA posts a copy of that certificate to the LDAP directory in a location in which the operator has identified the basic log-in rights and access rights for that individual to the CCLCMS system. Where one would typically have a log-in password type of implementation, the user is now identified by the stored certificate information instead of a log in password. Following the creation process of the card, the card is distributed out to the cardholder. The PINs for those cards are distributed through a separate mechanism for security in case the cards fall into an unauthorized party's hands. That is similar to what is done in the industry today, for example, with ATM cards or credit cards. For example, a cardholder's cash PIN for a credit card comes as a separate mailing from the card itself, which gives the users rights to the system.

Continuing with the card creation process for an embodiment of the present invention, other modes of creating certificates for systems are the badging station and the personalization portal, which are examples of systems that interact with the CCLCMS providing updates and changes to data that is maintained within the system. It is deemed prudent when use is made of external systems that interact with a host over the Internet, to require the same level of security that is provided for individual

users that have update rights to the system. Those systems are required to use certificate based authentication and secure channel communications, utilizing those same certificates to identify themselves, to establish the communication, and then to pass the information securely across the Internet. To do that, an embodiment of the present invention includes, for example, methods for storing keys, requesting a certificate, and storing the certificate on the system.

The badging stations for an embodiment of the present invention are held in secure offices within the security structure of a corporation. Those offices are deemed to be secure locations and can have the certificates stored simply on a computer disk. The security issue with that is that the private key for the certificate, which is the identification seed (although encrypted on the disk) is still sitting on a disk, and since the content of a disk is accessible by anyone that walks into the office, there is some level of risk that the information on the disk can be compromised. However, given the structure of the environment of a secure office, there is a minimal risk involved.

To implement this in an embodiment of the present invention, referring to Fig. 2, a standard system method called keystore encryptokey is utilized to create a dialog in which a user on a system can request a certificate. That request is sent up to the RA, which reviews and manually approves the request and generates a certificate. When manually approving the request, the RA also logs onto the arterium LDAP and creates a log-on equivalent for that system. Upon creating the certificate, the CA posts the certificate to the LDAP directory, and an email is sent back to the user who created the certificate request on the system. The user is then able to log back on and request that the certificate be downloaded and stored using the standard certificate storage methods. The system can then interact with the CCLCMS system.

In this aspect of an embodiment of the present invention, the user logs onto the PC using a traditional log-in password on the PC and has rights to operate a particular program on the particular PC based on the user's usage rights. An individual user logs in on the PC, and the certificate is utilized in conjunction with a specific program on the PC, so that the user must have rights to operate that program. Once that is in place, the user is able to create badges. During the process of creating badges, an update is provided back to the LCMS system indicating that certain badging cards have changed status. Administration for a card for an individual user has been previously mentioned in the context of a badging station, where the certificates are stored on the disk itself. The certificate is utilized by the badging program rather than

by an individual user, so any user that has rights to create badges also has rights to utilize the certificate. The certificate is tied to the program.

In a third instance, referring to Fig. 3, the process for requesting a certificate for an embodiment of the present invention is similar, except instead of storing the certificate on a disk, the request includes HSM processing. The request says, in effect, "I am going to create my own key pair using the HSM" and requests that the HSM create a public key pair and deliver only the public key external to it. There is a private key and a public key in a public key pair, and the HSM simply creates the pair and stores the private key, so there is no external disability whatsoever of the private key. The HSM then packages the public key with its request information and sends it up to the RA. The RA reviews and approves the request and creates the entry in the LDAP for the particular system user. The same process then occurs in which the CA receives the request, verifies its completeness, creates the certificate, and then posts an email back to the operator that was attached to the request. Once that email is received, the operator goes back online and downloads the certificate, which is the signed document using the CA's key pair, but only includes the public key.

That information is then deposited on the disk, but the private key in this case is always on the HSM. In today's Internet environment, HSMs are used with web servers, which is akin to the CCLCMS side of the equation here. However, HSMs have not been used to store a private key of the certificate on a client's side system. Referring further to the operation of the PC based, soft certificate storage, this certificate is tied to the use of a particular application. The application runs on a system that is operable continuously. It is not something that someone logs in and starts up. It provides the service unto itself. The personalization portal in the corporate badge aspect is a device that sits and runs continuously as a server to corporate cardholders to personalize the applications on the cardholder's card once the card is received by the cardholder.

The cardholder goes to a badging office for an embodiment of the present invention, and the badging office creates the card for the cardholder. The badging office also personalizes the card with some general information, photographs, and the like. However, when it comes to personalizing individual applets and services that are offered on the card, that is something that the cardholder does himself or herself. The cardholders customize the cards for themselves at their own office workstations. When they are doing that and changing the applet states on the card and actually

doing the personalization, it is necessary for the system to capture changes to the card's state, so that it knows what the configuration of the card looks like at any point in time. The personalization portal runs continuously and is available for use continuously. The certificate is tied to a particular application, and whenever a request comes in to personalize a card, if it requires any verifications or validations from the CCLCMS system or requires updating any information on the CCLCMS system, the certificate is once again used to authenticate that server to the CCLCMS system and then to create the secure channel and secure the communication for that transaction. A minor difference in its use is that it is not the logging in by the users that is activating the application.

Certificates by their nature have an expiration date, and rationales for the expiration date are, for example, to make sure that people are still utilizing them and that those people are still authorized. If administrators change and the like, they may want to clean up the database. In connection with having certificates age off, some sort of active processing is required to maintain a user on the system. Further, encryption technology continues to change, and sophistication of users that attempt to break into systems continues to grow. Therefore, over time, one wants to make sure to use whatever is the most current encryption technology in conjunction with the certificate, such that reasonable security is being provided to the system. For those kinds of reasons, certificates age, and an embodiment of the present invention provides different methods that can be utilized within the system to reissue certificates.

One method of reissuing certificates for an embodiment of the present invention is that by an automatic process near the termination of the certificate, a notification is posted to the system, so that the next time a user with the particular certificate logs in, the user is notified that the certificate is about to expire, and the user can proactively renew the certificate. Another process is that once the certificate has expired, the user can go back to the original request page through the RA, and utilizing the information that is currently on the user's card, the user can request a new certificate. Given that the request is for a user that has been validated within the system, there is a certain period of time in which those requests are automatically accepted and a new certificate issued and downloaded to the card, and the LDAP directory for that user is updated accordingly. Thus, there is continuous use of the system. During that time period, the user does not need to supply certificate

information. It is gleaned from the expired certificates, automatically issued, and requires no RA approvals.

Another aspect of reissuance is revocation of a certificate, again primarily using mechanisms that are in place within the CA environment. When a certificate is identified as revoked, the CA does certain things. One such thing is that the CA has the ability to create what is called a CRL, which is a Certificate Revocation List, add information to that list, and post that list to the system. That is the commonly utilized method for distributing certificate revocations to a public environment. The situation for an embodiment of the present invention is different in that the CA is used only to create access control authorizations for users of this system. The system has a shared LDAP directory to which the CA has access, as well as the host system itself.

Thus, when a certificate is revoked, the CA is allowed to pull that certificate information from the user access definition within the LDAP directory. By doing this, if a user then attempts to log on utilizing that certificate for the system, when the CCLCMS system goes to verify that the certificate is the one that is issued to the user, the information is not resident in the LDAP directory, thereby forcing a failure to authenticate and denial of a connection. This works with both the users and the systems. As soon as the certificate is revoked, there is literally an instantaneous posting of that removal of that information from the LDAP directory and therefore immediate disallowance of access to the system.

An embodiment of the present invention uses existing certificate-based authentication combined uniquely and delivering access rights or access methods for accessing the CCLCMS components of the system for users and systems with both soft and hard storage methods. An embodiment of the present invention provides unique methods for requesting, processing, and delivering the certificates, as well as a consistent approach for reissuance and revocation across various entities. Another important aspect is the actual request process for the client side systems that includes an HSM.

Various preferred embodiments of the invention have been described in fulfillment of the various objects of the invention. It should be recognized that these embodiments are merely illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be readily apparent to those skilled in the art without departing from the scope of the present invention.

What is claimed is: